AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Data extracted from a Samsung Galaxy Note II, currently located on an external drive stored in a storage locker located at 2100 Jamieson Ave. Alexandria, VA 22314

Case No. 1:19-sw-1134

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 793(c) (obtaining national defense information), 18 U.S.C. § 793(e) (retaining and transmitting national defense information), 18 U.S.C. § 793(e) (causing the communication of national defense information), 18 U.S.C. § 798(a)(3) (disclosing classified communication intelligence information), 18 U.S.C. § 641 (theft of government property).	

The application is based on these facts:

See Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Alexander P. Berrang

Laura Pino
Applicant's signature

Laura J. Pino, F.B.I. Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: August 22, 2019

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF DATA FORENSICALLY EXTRACTED FROM A SAMSUNG GALAXY NOTE II AND WHICH CURRENTLY IS LOCATED ON AN EXTERNAL DRIVE STORED IN A STORAGE LOCKER LOCATED AT 2100 JAMIESON AVENUE, ALEXANDRIA, VIRGINIA 22314

Case No. 1:19-SW-1134

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Laura J. Pino, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a Search Warrant authorizing the forensic examination of property—data forensically extracted from a Samsung Galaxy Note II (hereinafter, the "**TARGET DATA**"), which currently is in law enforcement possession and described further below and in Attachment A—for the electronically stored information described in Attachment B.

2. I am a Special Agent employed by the Federal Bureau of Investigation, and am assigned to the FBI's Baltimore Division. I am a graduate of the FBI Academy at Quantico, Virginia, and have extensive training in federal law. I have been employed by the FBI as a Special Agent for approximately 22 years, in which time I have investigated criminal violations relating to the mishandling of classified national defense information. I have directly participated in numerous investigations and search warrants involving the mishandling of

classified national defense information. I have received training in the area of handling classified information and have had the opportunity to observe and review examples of mishandled classified information in all forms of media, including computer media.

3. The information contained in this Affidavit is based on my personal knowledge and observations made during the course of this investigation, information conveyed to me by other U.S. Government employees, personal review of records, documents, and other physical evidence obtained during this investigation. This Affidavit contains information necessary to support probable cause. It is not intended to include each and every fact and matter observed by me or known to the U.S. Government.

4. This Affidavit is submitted for the limited purpose of showing probable cause to believe that the **TARGET DATA** contains evidence, fruits, contraband, and/or instrumentalities of the offenses described in Attachment B, in particular, obtaining national defense information, in violation of 18 U.S.C. § 793(c), retaining and transmitting national defense information, in violation of 18 U.S.C. § 793(e), causing the communication of national defense information, in violation of 18 U.S.C. § 793(e), disclosing classified communication intelligence information, in violation of 18 U.S.C. § 798(a)(3), and theft of government property, in violation of 18 U.S.C. § 641.

THE DATA TO BE EXAMINED

5. The **TARGET DATA** is data that the FBI extracted on August 9, 2014, from a Samsung Galaxy Note II and was reprocessed with a forensic application on July 31, 2019. As described further below, the FBI seized the Samsung Galaxy Note II on August 8, 2014, from DANIEL EVERTTE HALE's residence in Lorton, Virginia, which is within the Eastern District of Virginia, and pursuant to a search warrant issued the same day by the Honorable Thomas

Rawles Jones, Jr. A more complete description of the circumstances in which the **TARGET DATA** was acquired is provided in the next section.

6. The **TARGET DATA** currently is located in a locked, storage locker located at the U.S. Attorney's Office for the Eastern District of Virginia, 2100 Jamieson Avenue, Alexandria, Virginia 22314.

7. The applied-for warrant would authorize the forensic examination of the **TARGET DATA** for the purpose of identifying electronically stored data particularly described in Attachment B.

SUMMARY OF PROBABLE CAUSE

8. On March 7, 2019, a federal grand jury in the Eastern District of Virginia returned a five-count indictment against HALE. The indictment charged HALE with one count of § 793(c), two counts of § 793(e), one count of § 798(a)(3), and one count of § 641. Then, on May 9, 2019, the federal grand jury returned a superseding indictment that primarily modified the § 641 count. HALE has pleaded not guilty, and a jury trial has been set for December 16, 2019.

A. Background on Classified Information

9. I know from my training and experience that classified information is defined by Executive Order 13526, 75 Fed. Reg. 707 (Jan. 5, 2010) as information in any form that (a) is owned by, produced by or for, or under the control of the U.S. government; (b) falls within one or more of the categories of information set forth in the Executive Order; and (c) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security that the original classification authority can identify and describe.

10. I also know from my training and experience that under Executive Order 13526, the designation SECRET (S) shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. The designation TOP SECRET (TS) shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security. NOFORN stands for "No Foreign Dissemination" and denotes that dissemination of that information is limited to U.S. persons. ORCON stands for "Originator Controlled," which denotes that the information should not be further disseminated to any third party without the concurrence of the original classification authority.

11. Executive Order No. 13526 also provides that specified officials may create special access programs upon a finding that the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access applicable to information classified at the same level are not sufficient to protect the information from unauthorized disclosure. Special access programs pertaining to intelligence sources, methods, or analytical processes are called SCI programs. One such SCI control system is SI information, which refers to "Special Intelligence." SI protects information relating to technical and intelligence information derived from the monitoring of foreign communication signals by someone other than the intended recipients. The term COMINT describes communications intelligence.

12. Pursuant to Executive Order No. 13526, classified information generally can only be disclosed to those persons who have been granted an appropriate level U.S. government security clearance and who possess a valid need to know to perform a lawful and authorized government function. Additionally, classified information only may be processed and retained in

and on facilities approved for processing and storage at the appropriate classification level. Classified information may not be removed from official premises without proper authorization.

B. HALE's Misappropriation of Classified and Unclassified Documents from the National Geospatial-Intelligence Agency

13. Through my investigation, I have learned the following information about HALE:

a. HALE was enlisted in the U.S. Air Force from approximately July 2009 to July 2013. He received language and intelligence training, became a language analyst, and later was assigned to work at the National Security Agency (NSA) from approximately December 2011 to May 2013. HALE deployed in support of a Department of Defense Joint Special Operations Task Force from March 2012 to August 2012, at Bagram Airfield, Afghanistan, working for most of that time as an Intelligence Analyst responsible for identifying, tracking, and targeting threat networks and targets. In connection with his active duty service and work for NSA, HALE held a TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION (TS//SCI) security clearance, and had access to classified national defense information.

b. From approximately December 2013 to August 2014, HALE was employed by a defense contractor known as Leidos. While working for Leidos, HALE was assigned to the National Geospatial-Intelligence Agency (NGA), in Springfield, Virginia, where he worked as a Political Geography Analyst. HALE was required to receive and maintain a TOP SECRET//SCI security clearance in order to work at NGA.

c. Over his many years holding a security clearance, HALE received training regarding classified information, including the definitions of classified information, the levels of classification, and SCI, as well as the proper handling, marking, transportation, and storage of classified materials. HALE received training on his duty to protect classified materials from unauthorized disclosure, which included complying with handling, transportation, and storage

requirements. HALE knew that unauthorized removal and retention of classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials, and therefore could cause injury to the United States or be used to the advantage of a foreign nation. In particular, HALE had been advised that the unauthorized disclosure of TOP SECRET information reasonably could be expected to cause exceptionally grave damage to the national security of the United States, and unauthorized disclosure of SECRET information reasonably could be expected to cause serious damage to the national security of the United States, and that violation of the rules governing the handling of classified information could result in criminal prosecution.

d. HALE's work at NGA required the use of classified government computer systems and networks that provided access to classified national defense information. HALE was notified that these computers were monitored for "personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations" by a banner that HALE had to acknowledge by clicking on the "OK" button every time he logged on.

e. Because HALE held a security clearance and was assigned to NGA as a cleared defense contractor, the U.S. government entrusted HALE with access to closely held classified national defense information.

14. On August 7, 2014, NGA Security alerted the FBI that it had determined that HALE had printed U.S. government information from his U.S. government computer while at work at NGA in March and April 2014, and that some of this information was unrelated to his job at NGA, but connected to an FBI investigation regarding the leak of classified information. The FBI subsequently determined that HALE's user profile at NGA had been used to print 23 documents that were unrelated to his work at NGA. The FBI further determined that 17 of these

documents had been published in whole or in part: (a) in a series of articles that were written by, or contributed to by, a particular reporter (hereinafter, the "Reporter") and that were released via a particular, online news organization (hereinafter, the "Online News Organization"), and (b) in a book authored by the Reporter.

15. The table displayed below lists the 23 printed documents unrelated to HALE's work at NGA, the dates of printing, initial publication dates, and classifications:

Document	Date Printed	Date of Initial Publication	Classification
A	February 28, 2014	October 2015	SECRET
B	February 28, 2014	October 2015	SECRET
C	February 28, 2014	October 2015	SECRET
D	February 28, 2014	October 2015	SECRET
E	February 28, 2014	October 2015	TOP SECRET
F	February 28, 2014	October 2015	SECRET
G	April 3, 2014	April 2015	TOP SECRET
H	April 19, 2014	N/A	TOP SECRET
I	April 20, 2014	August 2014	SECRET
J	April 20, 2014	December 2015	SECRET
K	April 20, 2014	April 2015	TOP SECRET
L	April 30, 2014	July 2014	UNCLASSIFIED
M	May 14, 2014	August 2014	SECRET
N	May 14, 2014	August 2014	UNCLASSIFIED
O	May 15, 2014	December 2016	UNCLASSIFIED
P	May 15, 2014	December 2016	UNCLASSIFIED
Q	May 15, 2014	December 2016	UNCLASSIFIED
R	May 15, 2014	December 2016	UNCLASSIFIED
S	June 20, 2014	N/A	SECRET
T	June 27, 2014	N/A	UNCLASSIFIED
U	July 31, 2014	N/A	SECRET
V	August 5, 2014	N/A	SECRET
W	August 5, 2014	N/A	UNCLASSIFIED

16. I know from this investigation that 11 of the 17 published documents were marked as SECRET or TOP SECRET. I further know that the relevant original classification

authorities have since determined that these documents were correctly marked at the appropriate classification level at the time they were printed, and that they remain classified at the same level today.

17. On August 7, 2014, NGA Security searched HALE's workspace. NGA Security did not find any of the aforementioned documents in HALE's workspace. In fact, the search revealed that there were no personal effects in HALE's workspace, most likely due to his scheduled separation from NGA on August 8, 2014.

18. According to NGA, there is no evidence that HALE sought or received permission to remove or disclose classified information from NGA offices. Further, there is no evidence that HALE sought or received permission to access classified information outside his official area of responsibility, nor that he was assigned duties that would make access to such information necessary to accomplish his officially authorized government function.

C. Search of HALE's Residence

19. The FBI identified information on the Internet that connects HALE to the Reporter. In particular, the FBI found a February 2014 article by the Reporter and others that contained quotes from a "former drone operator for the military's Joint Special Operations Command . . . who also worked at NSA." This description matches HALE's work history, and accords with a November 2013 event organized by CODEPINK at which HALE told the audience, among other things, that he worked with unmanned drones while in the military.

20. The FBI also found a video clip depicting the Reporter at a bookstore in Washington, D.C., discussing a book he had written and a film about the book. The event appears to have occurred on June 8, 2013, and the Reporter can be seen sitting on a stage with two other individuals, one of whom appears to be HALE.

21. On August 8, 2014, Judge Jones issued search warrants for HALE's residence, motorcycle, and person. The warrants, in sum, authorized the search and seizure of evidence, fruits, and instrumentalities of the communication of national defense information, the unauthorized removal and retention of classified documents or material, and exceeding authorized access to government computers, in violation of 18 U.S.C. §§ 793(e), 1030(a)(1), 1030(a)(2)(B), and 1924. Cells phones were specifically enumerated as being subject to seizure.

22. The FBI executed these warrants on August 8, 2014, in Lorton, Virginia. As a result of the FBI's search, electronic devices were seized from HALE's residence. The FBI forensically imaged and examined these devices, and determined that HALE possessed Document T on his home computer and possessed a thumb drive that contained one page of Document A marked "SECRET" in deleted space.

23. One of the items seized from HALE's residence was a Samsung Galaxy Note II, which the FBI found in his bedroom. The Samsung Galaxy Note II subsequently was transported to an FBI facility in Maryland.

D. The Forensic Extraction and Examination of the Samsung Galaxy Note II

24. On August 9, 2014, an FBI computer forensic examiner used a forensic tool to extract data from the Samsung Galaxy Note II. This extraction, in other words, is the source of the **TARGET DATA**. The computer forensic examiner saved the **TARGET DATA** to a compact disc, and loaded the **TARGET DATA** into a forensic review platform, which I then used to review the extracted data.

25. My review of the data extracted from the Samsung Galaxy Note II revealed several communications of note, including the following:

a. On or about May 23, 2013, HALE sent a text to another individual stating "[the Reporter] wants me to tell my story about working with drones at the opening screening of his documentary about the war and the use of drones."

b. Following the June 8, 2013 event at which HALE sat next to the Reporter, HALE texted another individual that he was "with [last name of the Reporter]" and was "headed to a" restaurant in Washington, D.C.

c. On or about July 14, 2013, HALE called a number that, at one time, had been saved in his phone under the first name of the Reporter. Three days later, HALE called this number again. I will refer to this telephone number herein as the "Reporter's Number."

d. On or about July 19, 2013, HALE sent a text message to another individual stating that he was going to New York "to meet with [first name of the Reporter]," another person (presumably a journalist), and "some other journalist."

e. On or about August 18, 2013, HALE received a call from the Reporter's Number, which lasted approximately 35 minutes.

f. In November 2013, HALE sent a text message to the Reporter's Number, asking whether the Reporter would "be in D.C. this weekend for the anti drone summit."

g. On or about February 27, 2014, HALE sent a text message to the Reporter's Number, asking, "Are you able to get on chat?"

h. On or about February 28, 2014, approximately four hours after using his classified work computer at NGA to print Documents A through F, HALE sent messages to, and received messages from, the Reporter's Number. They were as follows:

HALE: Can you be here Monday?

The Reporter: Where?

The Reporter: I am out in LA for oscars. Back Tuesday.

HALE: Right, I understand, do you have time to stop by DC?

The Reporter: Let me see if I can change flight.

HALE: Please do and lemme know.

26. The Samsung Galaxy Note II and the CD on which the **TARGET DATA** was saved, remain in the lawful possession of the FBI. Moreover, HALE has not requested the return of any of his property, including the Samsung Galaxy Note II.

27. I know that the forensic application used in 2014 to review the **TARGET DATA** has been updated in the intervening five years. On July 31, 2019, a computer forensic examiner with the FBI used the latest version of the aforementioned forensic application to determine whether advancements in technology would result in the application making more of the **TARGET DATA** human readable. The computer forensic examiner has advised that the latest version of the forensic application appears to be able to parse additional data. This is because, after using the latest version of the application to process the **TARGET DATA**, there appears to be at least more contacts and text messages available for review than when the **TARGET DATA** was processed by the 2014 version of the application. The computer forensic examiner has advised that, after she reprocessed the **TARGET DATA**, the application displayed a summary screen that provided statistics on the types of data that had been parsed, such as the number of contacts. The computer forensic examiner also has advised that she reviewed only the portion of the reprocessed data that relates to the contacts on the Samsung Galaxy Note II and did so to verify that the Reporter's Number had been parsed. Conversely, I have not reviewed any portion of this newly re-parsed, human-readable data.

28. While the FBI might already have all necessary authority to examine the **TARGET DATA**, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **TARGET DATA** will comply with the Fourth Amendment and other applicable laws.

29. The **TARGET DATA** is currently in storage at a locked, storage locker located at the U.S. Attorney's Office for the Eastern District of Virginia, 2100 Jamieson Avenue, Alexandria, Virginia 22314. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **TARGET DATA** first came into the possession of the FBI.

TECHNICAL TERMS

30. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. ***Wireless telephone.*** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal

calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (GPS) technology for determining the location of the device.

b. ***Digital camera.*** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images usually can be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. ***Portable media player.*** A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. ***GPS.*** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. GPS

consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals use specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives these signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision which provide the location of the device.

e. ***PDA.*** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. ***IP Address.*** An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is,

long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. ***Internet.*** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

31. Based on my training, experience, and research, I know that a Samsung Galaxy Note II has capabilities that allow it to be used to access the Internet and to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, as well as how the device was used.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. There is probable cause to believe that things that were once stored on the Samsung Galaxy Note II may still be stored within the **TARGET DATA**, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, digital storage media—in particular, digital devices' internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. ***Forensic evidence.*** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Samsung Galaxy Note II was used, the purpose of its use, who used it, and when. There is

probable cause to believe that this forensic electronic evidence might be within the **TARGET DATA** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals and the times the device was in use. Digital device file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to transmit documents or information about classified, national defense information or misappropriated unclassified government documents, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

35. ***Nature of examination.*** Based on the foregoing, and consistent with Rule 41, the Warrant I am applying for would permit the examination of the **TARGET DATA** consistent with the Warrant. Markedly, I am not requesting authority to extract data anew from the Samsung Galaxy Note II; rather this Application, out of an abundance of caution, requests authorization to use an updated forensic tool to review data that already has been extracted and is in the lawful possession of the United States.

//

//

//

CONCLUSION

36. I submit that this affidavit supports probable cause for a Search Warrant authorizing the examination of the **TARGET DATA** described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Laura J. Pino, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 22nd day of August, 2019:

/s/ JFA
John F. Anderson
United States Magistrate Judge

The Honorable John F. Anderson
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The **TARGET DATA** is data that the FBI extracted on August 9, 2014, from a Samsung Galaxy Note II—which the FBI seized on August 8, 2014, from DANIEL EVERTTE HALE's residence in Lorton, Virginia, which is within the Eastern District of Virginia, pursuant to a Search Warrant issued the same day by the Honorable Thomas Rawles Jones, Jr.—and that was reprocessed with a forensic application on July 31, 2019.

The **TARGET DATA** currently is located at a locked, storage locker located at the U.S. Attorney's Office for the Eastern District of Virginia, 2100 Jamieson Avenue, Alexandria, Virginia 22314. This warrant authorizes the forensic examination of the Target Data for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records within the **TARGET DATA** described in Attachment A that relate to violations of 18 U.S.C. § 793(c) (Obtaining National Defense Information), 18 U.S.C. § 793(e) (Retaining and Transmitting National Defense Information), 18 U.S.C. § 793(e) (Causing the Communication of National Defense Information), 18 U.S.C. § 798(a)(3) (Disclosing Classified Communication Intelligence Information), and 18 U.S.C. § 641 (Theft of Government Property), and involve Daniel Everette Hale, including:

a. Records or information relating to the theft, retention, transmission, disclosure, or communication of U.S. government documents, including classified, national defense information and unclassified documents;

b. Records or information relating to the publication of U.S. government documents, including classified, national defense information and unclassified documents;

c. Records or information pertaining to Hale's schedule or travel;

d. All bank records, checks, credit card bills, account information, and other financial records;

e. Photographs relating to the criminal conduct identified above, or that would reveal the identity or relationships between Hale and individuals to whom he disclosed or communicated U.S. government documents, including classified, national defense information and unclassified documents;

2. Evidence of who used, owned, or controlled the Samsung Galaxy Note II described in Attachment A at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, chat or instant messaging logs, photographs, and correspondence;

3. Records of Internet Protocol addresses used;

4. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. Evidence of software that would allow others to control the Samsung Galaxy Note II, such as viruses, Trojan horses, and other forms of malicious software;

6. Evidence of security software designed to detect the types of malicious software described above;

7. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

8. Evidence indicating how and when the Samsung Galaxy Note II was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

9. Evidence of the attachment of the Samsung Galaxy Note II to a computer, wireless telephone, or other electronic device or storage media;

10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Samsung Galaxy Note II;

11. Evidence of the times the Samsung Galaxy Note II was used; and

12. Contextual information necessary to understand the evidence described in this Attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.